CHAPTER 13

MAINTAINING AND UPGRADING A NETWORK

After reading this chapter and completing the exercises, you will be able to:

- Perform a baseline analysis to determine the state of your network
- Plan and follow regular hardware and software maintenance routines
- Describe the steps involved in upgrading network operating system software
- Describe the steps involved in adding or upgrading network hardware
- Address the potential pitfalls of making changes to the network
- Research networking trends to plan future network upgrades

ON THE JOB

I once worked in the computer services department of a world-class opera house and theater. Two years ago it became clear that our needs had outgrown our network. Users experienced slow responses and frequent down time, and the networking professionals found it difficult to support the outdated equipment. It was time for an upgrade.

We found the financing to completely overhaul our network, from backbone to desktop. We enlisted a consulting firm to help us plan this undertaking. Because the project was so large (affecting every bit of our operation, from Marketing to Payroll), the consultants recommended dividing the conversion into phases that would be less disruptive: backbone upgrade, LAN cabling, network device migration, desktop migration, and documentation and maintenance. One of the most difficult tasks was recabling our facility—a building that didn't resemble your average office building. Nevertheless, over a period of six months, and with help from several contractors, we completed the entire project.

The new network allows the theater's staff to work more efficiently. The network handles data more quickly and almost never suffers down time. And I now work for the consulting company that performed the upgrade!

Sophie Harris
Sage Systems

A network, like any other complex system, is in a constant state of flux. Whether the changes are due to internal factors, such as increased demand on the server's processor, or external factors, such as the obsolescence of a certain model of hub, you should count on spending a significant amount of time investigating, performing, and troubleshooting changes to your network. In Chapter 12, you learned how to find and resolve problems on a network. Some of the solutions discussed there required changes to software or hardware. In this chapter, you will build on this knowledge to learn about changes dictated by immediate needs as well as those required to enhance the network's functionality, growth, performance, or security.

Ideally, you will plan and budget for all changes to your network. In reality, however, many network changes result from sudden, unexpected requirements. For example, a security breach at your organization might prompt the Vice President of IT to declare that all firewall operating systems must be upgraded and that all system access permissions must be scrutinized. To accomplish these quick changes, you must possess excellent technical skills, understand your network thoroughly, and think fast. Upgrading firewalls is one small example of a network enhancement that you need to properly plan and test. In this chapter, you will learn about a variety of ways to maintain and upgrade your network so as to make it more secure, reliable, and responsive.

KEEPING TRACK

As you learned in Chapter 12, keeping accurate and updated documentation on every aspect of your network will facilitate troubleshooting and help you manage your network more effectively. With network maintenance tasks, you should track all changes and upgrades you perform. You should also note the state of the network before and after you implement any modifications. The first topic in this section, baselining, suggests how to begin this process of documentation.

Baselining

The first step in properly maintaining your network is to identify its current state. You cannot predict how a network will perform in the future until you have analyzed its past performance. The practice of measuring and recording a network's current state of operation is called **baselining**. Baselining measurements may include the utilization rate for your network backbone, number of users logged on per day or per hour, number of protocols that run on your network, statistics about errors (such as runts, collisions, jabbers, or giants, described in Chapter 12), frequency with which networked applications are used, or information regarding which users take up the most bandwidth. Figure 13-1 shows a graph that provides a baseline for daily network traffic over a six-week period.

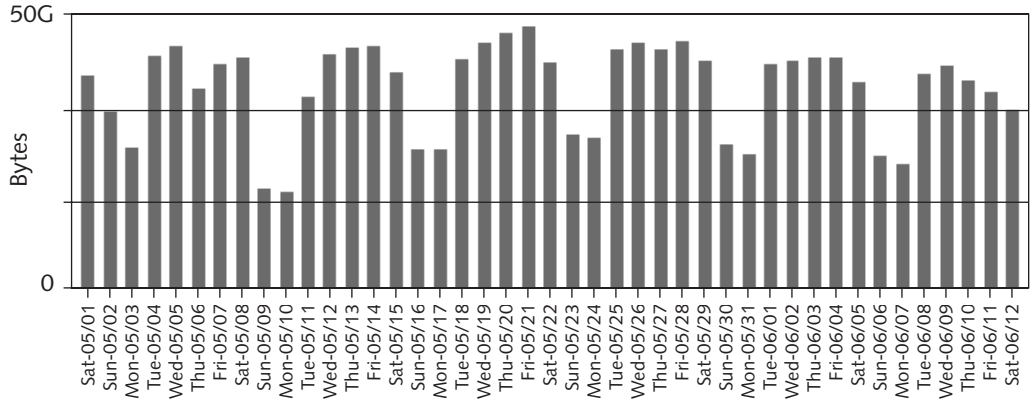

Figure 13-1 Baseline of daily network traffic

Each network will require its own baselining approach. The elements you measure will depend on which functions are most critical to your network and its users. If your staff members run the Lotus Notes application from their local hard disks, for example, but need to post the data they generate through queries to the Internet, you will probably be most concerned about the utilization rate of your gateway, rather than that of your server.

Baseline measurements allow you to compare future performance increases or decreases caused by network changes with past network performance. Baselining is the only way to know for certain whether your upgrades or changes help or harm your level of service.

For example, imagine that you have just added a new switch for the shared workstations in your organization's Customer Service department. Your manager wants you to prove that the switch is really worth the money she paid for it. If you have previously baselined the Customer Service department's network segment in terms of utilization and response time, you can measure the same characteristics after you install the switch and demonstrate how much more rapidly the users receive their data off the network. If the response time becomes worse, you will know that you probably configured or installed the switch improperly.

In another example, suppose that a group of users from the corporate headquarters complains about slow response time over the WAN. If you have baselined the characteristics of that WAN link, you can determine whether their slow response reflects higher-than-normal traffic or whether traffic is excessive and possibly caused by a network error.

In addition, baselining can help you predict the impact of a significant network change. When you are planning system upgrades, it provides the best way to predict your needs. For instance, suppose that your network currently serves 500 users and that your backbone traffic exceeds 50% at 10:00 A.M. and 2:00 P.M. each business day. That pattern constitutes your baseline. Now suppose that your company decides to add 200 users who

perform the same types of functions on the network. The added number of users equals 40% of the current number of users (200/500). Therefore, you can predict that your backbone's capacity should increase by approximately 40% to maintain your current service levels.

Network traffic patterns are notoriously difficult to forecast, because you cannot predict users' habits, the effects of new technology, or changes in demand for resources over a given period of time. For instance, the preceding example assumed that all new users would share the same network usage habits as the current users. In fact, however, the new users may generate a great deal more, or a great deal less, network traffic.

Baselining may help you decide how to accommodate capacity increases. For example, determining which, if any, groups of users generate the most network traffic can help you decide whether to upgrade the network from 10-Mbps to 100-Mbps Ethernet, whether to upgrade only certain segments of the network, or whether to manage the increase by adding switches and further subnetting the network.

How do you gather baseline data on your network? Although you could theoretically use a network monitor or network analyzer and record its output at regular intervals, several programs can perform the baselining for you. These programs range from freeware available on the Internet to expensive, customizable hardware and software combination products.

Before choosing a network baselining tool, you should determine how you will use it. If you manage a small network that provides only one critical application to users, an inexpensive tool may suffice. If you work on a WAN with several critical links, however, you should investigate purchasing a more comprehensive program. Look for a program with a familiar and easy-to-use interface, preferably one that provides templates and wizards to enable you to set your measurement parameters quickly. Make sure that the tool can be integrated with your operating system environment and that it supports the networking hardware used by your organization.

The baselining tool should also be capable of measuring the statistics needed. For example, only a sophisticated baselining tool can measure traffic generated by each node on a network, filter traffic according to types of protocols and errors, and simultaneously measure statistics from several different network segments.

In most cases, baselining tools record the information they collect in common database formats that enable you to generate reports and graphs depicting the health of your network. Examples of popular baselining tools include Concord Communications' Network Health, NetScout Systems' NetScout Manager Plus, and Wandel and Goltermann's WG Wizard.

Once you have identified the network statistics critical for your organization, chosen a baselining tool, and completed the initial baselining, you should set a regular schedule for reevaluating your network. You may want to perform baselining after any major network change or according to dates on the calendar. Regardless of which option you choose, regularly repeating the baseline measurements is the only way to establish a history of your network's performance. By creating such a history, you can identify trends and predict future needs.

Asset Management

Another key component in the evaluation of your network is identifying and tracking the hardware and software on your network, a process called **asset management**. The first step in asset management is to take an inventory of each node on the network. This inventory should include not only the total number of components on the network, but also each device's configuration files, model number, serial number, location on the network, and a technical contact for support. In addition, you will want to keep records of every piece of software purchased by your organization, its version number, vendor, and technical support contact.

As with a baselining tool, the asset management tool you choose will depend on your organization's needs. You may purchase a program that can automatically discover all devices on the network and then save that information in a database, or you may use a simple spreadsheet to save the data. In either case, your asset management records should be comprehensive and accessible to all personnel who may become involved in maintaining or troubleshooting the network. In addition, you should ensure that the asset management database is regularly updated, either manually or automatically, as changes to network hardware and software occur. The information you retain is useful only while it is current.

Asset management simplifies maintaining and upgrading the network chiefly because you know what the system includes. For example, if you discover that a router purchased two years ago requires an upgrade to its operating system software to fix a security flaw, you need to know how many routers are installed, where they are installed, and whether any have already received the software upgrade. An up-to-date asset management system allows you to avoid searching through old invoices and troubleshooting records to answer these questions.

In addition, asset management provides network administrators with information about the costs and benefits of certain types of hardware or software. For example, if you conclude that 50% of your staff's troubleshooting time is spent on one flawed brand of NIC, an asset management system can reveal how many NICs you would need to replace if you chose to replace those cards, and whether it would make sense to replace the entire installed base. In addition, some asset management programs can track the length of equipment leases and alert network managers when leases will expire.

The term "asset management" originally referred to an organization's system for keeping tabs on every piece of equipment it owned. This function was usually handled through the Accounting department. Some of the accounting-related tasks included under the original definition for asset management, such as managing the depreciation on network equipment or tracking the expiration of leases, apply to asset management in networking as well.

Change Management

In Chapter 12, you learned about using a change management system to track every modification you make while troubleshooting a network problem. You should also use your change management system to record any changes resulting from network maintenance or upgrades. In general, updating your change management system regularly will alert your colleagues of changes you've made and help you remember when you instituted them. This type of system will also enable you to correlate additions, removals, or changes in network components with differences in the network's performance. This benefit may simplify the process of taking baseline and network performance measurements.

Like asset management systems, change management systems are useful only if they are kept current. Unlike asset management records, however, change management records cannot be created by a program that automatically discovers hardware and software on the network. Instead, you (or your fellow network administrators) must supply information regarding when, why, and how changes occur.

SOFTWARE CHANGES

If you have ever supported desktop computers professionally or even maintained your own computer at home, you know that an important part of keeping a system running optimally is upgrading its software.

You are most likely to implement the following types of software changes on your network: patches (improvements or enhancements to a particular piece of a software program), upgrades (major changes to the existing code), or revisions (a general term for minor or major changes to the existing code). Although the specifics vary for each type of software change, the general steps involved can be summarized as follows:

1. Determine whether the change (whether it be a patch, revision, or upgrade) is necessary.
2. Research the purpose of the change and its potential effects on other programs.
3. Determine whether the change should apply to some or all users and whether it will be distributed centrally or machine-by-machine.

4. If you decide to implement the change, notify system administrators, help desk personnel, and users. Schedule the change for completion during off-hours (unless it is an emergency).
5. Back up the current system or software before making any modifications.
6. Prevent users from accessing the system or part of the system being altered (for example, disable logins).
7. Keep the upgrade instructions handy and follow them during installation of the patch or revision.
8. Make the change.
9. Test the system fully after the change, preferably exercising the software as a typical user would. Note any unintended or unanticipated consequences of the modification.
10. If the change was successful, reenable access to the system. If it was unsuccessful, revert to the previous version of the software.
11. Inform system administrators, help desk personnel, and users when the change is complete. If you had to reverse it, explain why.
12. Record your change in the change management system.

As a general rule, upgrading or patching software according to a vendor's recommendations is a good idea and can often prevent network problems. For example, a vendor may issue an alert to its customers regarding a security flaw in its Web browser product. To fix this flaw, it may supply a patch. At other times, you may have to search for product upgrades on your own. Whatever your means of finding patches and upgrades, you should take responsibility for this task and make the necessary changes to your network's software. Bear in mind, however, that such changes can sometimes create even more trouble on your system. You should therefore be prepared to reverse software upgrades or patches, just in case.

In the following sections, you will learn about the types of software changes associated with sensible network maintenance. You will also see the best way to approach these changes.

Patches

As mentioned earlier, a **patch** is a correction, improvement, or enhancement to a particular piece of a software program. It differs from a revision or software upgrade in that it changes only part of a software program, leaving most of the code untouched. Patches are often distributed at no charge by software vendors in an attempt to fix a bug in their code or to add slightly more functionality.

You'll encounter patches in all areas of routine networking maintenance. Among other things, network maintenance sometimes requires patching the server's network operating system. For example, if your server runs NetWare 5.x, you may need to patch it to enable it to act as a reliable NAT router. A Windows 2000 server might require similar patches or perhaps something quite different.

Microsoft calls its significant patches for Windows 2000 Server "**service packs**." You may see them abbreviated as "SP1" and "SP2" for Service Pack 1 and Service Pack 2, respectively.

Keep in mind that a patch is not a replacement for an entire software package; instead, a patch is installed on top of the existing software. Patches apply to more than just network operating system software. For example, you might have to patch the software on your Cisco switch to allow it to handle IP multicasts over a Token Ring network. Alternatively, you might patch the program that allows you to centrally control your printers across the network.

If you install new hardware on a Windows 2000 server after installing a service pack, you will be prompted to insert your original Windows 2000 installation CD to obtain the device driver and support files for that hardware. By doing so, however, you may overwrite some of the files that were updated by the service pack. Therefore, it is a good idea to upgrade your server's hardware *before* applying service packs. If you do upgrade the server's hardware after installing a service pack, you may have to implement the service pack a second time.

Patch installations are no more difficult than installations of new software programs. The patch itself should come with installation instructions and a description of its purpose, at the very least, in the form of a text file. As with any significant system change, you should back up the system before installing a patch. Although patches ought to be fully tested by the vendor before release, you cannot assume that they will work flawlessly on your system. This consideration is especially important when you are patching network operating system software. Although some patch programs will automatically make a backup of the system before installation begins, you should not rely on this method. Always make sure you have a way to reverse a software change if it does more harm than good.

In addition, try to perform software patches during a time when users cannot and will not attempt to access the network. Even if you suspect that a patch can be implemented quickly and without adverse effects on current users, don't take a chance by applying it during normal business hours. If the patch does create problems, you will need extra time to reverse the process. Depending on how complicated or comprehensive the patch is, you may want to alert users to stay off the system for only a few hours or perhaps overnight.

After applying the patch, test the system to verify that its desired enhancements have taken effect. At this time, you should review the vendor's documentation to ensure that

you have correctly understood the patch's purpose and installed it correctly. For some patches to take effect, you will have to change system configuration files and restart the system. Test the software to verify that the patch hasn't caused any unintentional, undesired effects. Once you are certain that the patch worked successfully, you can allow users to access the system again.

To stay apprised of patches released by your vendors, you should regularly check the vendor's technical support Web site or subscribe to its mailing list. Manufacturers will usually attempt to bundle a number of bug fixes into one large patch; if you're a registered user, they will alert you about the release of significant patches. News about patches from vendors as large as Novell and Microsoft will also probably appear in trade magazines. Smaller vendors may need to release a patch that fixes a single problem with their program only occasionally.

Make it a policy to keep informed about patches to your network software, whether it involves the operating system, an application, or a client program. If you work in a large organization with several servers, routers, and other devices, you may want to assign one network administrator to manage patches for the servers, one to manage patches for the printers, and so on.

Client Upgrades

As you are probably aware, a software **upgrade** is a major change to a software package's existing code. An upgrade may or may not be offered free from a vendor and may or may not be comprehensive enough to substitute for the original program. An upgrade to the client program replaces the existing client program. In general, upgrades are designed to add functionality and fix bugs in the previous version of the client. For example, Microsoft's technical support site offers an upgrade for the Windows 2000 operating system that improves its level of encryption to provide better security. On a Novell client, you might perform an upgrade that enables clients to take advantage of the new features in NetWare 5.1. The scope and purpose of client upgrades vary widely, depending on whether the upgrade is a redesign or simply a bug fix.

The term **bug** is frequently used to describe a flaw in a software program that causes some part of the program to malfunction. Less frequently, this term may also be used to describe a hardware defect. Legend has it that the term originated when a moth became trapped inside the electrical workings of the first digital computer.

Before upgrading client software, carefully read the instructions accompanying the upgrade. It should reveal how to best install the software, whether the upgrade requires you to first install any previous upgrades, whether the upgrade requires any special preparation, and how its changes will affect users.

A client upgrade may be transparent to users, or it may completely change the appearance of the network login interface. Client upgrades typically overwrite some system files (such as .dll files) on the workstation, so their installation may affect other programs

adversely. They may even prevent other programs from working as they did in the past. For example, a user who receives an upgrade to his or her Windows 98 Dial-up Networking client may later experience problems with an older version of AOL software that worked perfectly for the last two years. In this case, the best solution may be to upgrade the AOL software as well.

As with all upgrades, you should test a client upgrade on a single workstation before distributing it to all users. Also, you should prepare a way to reverse the process. Because most client upgrades do not back up the previous version automatically, you should keep the old client software close at hand, either on the network or on disk, in case you need to reinstall it.

You may either perform client upgrades on a workstation-by-workstation basis or use a software distribution program such as Microsoft's Systems Management Server to upgrade multiple workstations simultaneously from the network. Although the latter approach is more efficient, it may not be appropriate in all situations. Consider a network of 500 users who have different software, hardware, and usage requirements. Can you be certain that the client upgrade will be compatible with each workstation's hardware and software? Can you be certain that the client upgrade will not adversely affect any user's current software setup? Can you be certain that every user will log in to the network to receive his or her upgrade? (For instance, what happens if many users are mobile?)

In general, you need to plan carefully and become familiar with your client characteristics before allowing a software distribution program to upgrade client software. In addition, you should notify clients about the upgrade and explain how their workstation might change as a result. If you don't, users may become alarmed at the changes and flood the help desk with questions.

Application Upgrades

Like client upgrades, application upgrades represent modifications to all or part of a program that are designed to enhance functionality or fix problems related to software. Application upgrades, however, apply to software shared by clients on the network. Bear in mind that changes to shared applications will affect all users at once. You should therefore take extra precautions to ensure that the application upgrade does not cause unanticipated problems. It's essential to test it fully before allowing users to access the new version.

The principles underlying the modification of shared applications on the network are the same as those for the modification of client software. Before applying the change, you should determine the need for it and its potential effects. You should also back up the current software before upgrading it, prevent users from accessing the software during the implementation process, and keep users and system administrators informed of all changes.

Unlike client or system software upgrades, application upgrades are not usually designed to fix problems in the software, but rather to enhance the program's functionality. For this reason, an application upgrade may be more a matter of convenience than necessity. Therefore, the time, cost, and effort involved in application upgrades should be weighed against the necessity of performing operating system or client upgrades. This consideration is especially important if a networking professional's time is limited (as it usually is). For example, users may urge a network administrator to upgrade the company's version of WordPerfect. If the only advantage in doing so is to allow users to print watermarks on their labels, the upgrade may be a waste of time and money. On the other hand, if the application upgrade will add a necessary feature, such as integration with the company's messaging system, it may be well worth the effort.

For a significant application upgrade, you may also need to provide (or suggest classes for) user training. If you choose to refer your users to an outside training facility, make sure they will learn about the particulars of the application in your networking environment. For instance, if you make it a policy never to install the sample spreadsheets for a Lotus 1-2-3 program, make sure your users know about this constraint. Likewise, if you have limited the functionality of a program (for example, preventing users from posting the Web pages they create in Microsoft FrontPage to the server), you should publicize this policy. The better you prepare and inform your users, the fewer support calls your help desk will have to field.

Network Operating System Upgrades

Perhaps the most critical type of software upgrade you'll perform is an upgrade to your network operating system. It usually involves significant, potentially drastic, changes to the way your servers and clients operate. As such, it requires plenty of forethought, product research, and rigorous testing before you implement it. In fact, for any network with more than a few users, you should create and follow a project plan for this undertaking. This plan should include all of the precautions typically associated with other software upgrades. In addition, you should consider the following in your project plan:

- How will the upgrade affect user IDs, groups, rights, and policies?
- How will the upgrade affect file, printer, and directory access on the server?
- How will the upgrade affect applications or client interactions on the server?
- How will the upgrade affect configuration files, protocols, and services running on the server?
- How will the upgrade affect the server's interaction with other devices on the network?
- How accurately can you test the upgrade software in a simulated environment?
- How can you take advantage of the new operating system to make your system more efficient?

- What is your technical support arrangement with the operating system's manufacturer if you need help in the midst of the upgrade?
- Have you allotted enough time to perform the upgrade (for example, would it be more appropriate to do it over a weekend rather than overnight?)?
- Have you ensured that the users, help desk personnel, and system administrators understand how the upgrade will affect their daily operations and support burdens?

The preceding items are only some of the critical questions you need to ask before embarking on a network operating system upgrade. Your networking environment may warrant additional considerations. For example, suppose that you are the network administrator for a company that is merging with a second company. Your two companies may use dissimilar network operating systems, and the IT Director may ask you to upgrade your network's operating system to match the other company's version. In this situation, you would have not only the previous list of questions to consider, but also a list of questions pertaining to the other company's operating system. For instance, how are its NOS directories organized? By addressing these questions before you upgrade your own network operating system, you will ensure that the merger of the two networks goes more smoothly.

A network operating system upgrade is a complex and far-reaching change. It should not be undertaken with severe budgetary, resource, or time constraints. The following scenario illustrates how careful planning and a methodical process can help you accomplish a network operating system upgrade. In this scenario, a network administrator performs an exemplary network operating system upgrade.

Tom is the network administrator for an accounting firm that employs 400 full-time staff members and uses three NetWare 4.11 servers. Tom is considering upgrading the servers to NetWare 5.1. He has read about the benefits of NetWare 5.1 and thinks his organization may be outgrowing its NetWare 4.11 servers. In addition, his colleagues and a few of his knowledgeable users have been asking when the servers will be upgraded. Tom decides to make the upgrade one of his priorities. He delegates some of his other tasks to co-workers and gets to work.

1. Research—Tom gathers the trade magazine articles he's seen about NetWare 5.1. Because he knows that trade magazine articles can be inaccurate or biased, he also searches Novell newsgroups on the Internet to find out what network administrators who have performed a similar upgrade report about their experiences. He calls a trusted local consultant to ask her advice. In addition, Tom searches through Novell's Web site to see if the features provided by NetWare 5.1 are needed for his network and users. Finally, he finds out how much the software will cost. Once he has collected this information, Tom summarizes it in an outline form, just as if he were writing a term paper. In his outline, he lists the benefits and risks involved in embarking on this network operating system upgrade.

2. Proposal—Tom's initial research indicates that installing NetWare 5.1 would solve a number of technical problems, not to mention simplifying the centralized management of the company's 400 computers. Based on his research outline, Tom writes a proposal to evaluate the product, including a plan to purchase and implement NetWare 5.1 if his proposal is accepted. His proposal includes the following elements:
   - Questions to answer during evaluation (for example, "Can NetWare 5.1 work with my current network monitoring software?")
   - Names of personnel who will assist with evaluation and final approval
   - A rough timeline and plan for implementing the change if it is approved
   - A rough project plan for implementing the change if it is approved
   - Cost considerations
   - A review of the short- and long-term benefits of the upgrade
   - A review of the risks involved in the upgrade
   - A recommendation for or against performing the operating system upgrade
   - A plan for purchasing the software and implementing the change
3. Evaluation—Assuming that Tom's proposal concluded that his firm should proceed with an upgrade and that his superiors approved his recommendation, Tom is ready to begin the evaluation phase. He orders an evaluation copy of NetWare 5.1 from his Novell sales representative. He installs the software on an old server that is currently unused, but whose hardware is similar to the hardware of his three production servers (making sure that his servers meet Novell's recommended hardware requirements). On this system, he creates several mock user IDs and groups to simulate the real network environment. Tom also installs all of the applications and services that the server will support if it goes into production.

   Tom distributes updated client software to his team of engineers and asks them to use the mock IDs and groups to test the system. Over a given time period, they test the system and keep notes on how the system meets the requirements specified in Tom's proposal. The engineers pay particular attention to the new user interface for clients, the way in which their company's critical applications operate, the system's response time, and any new features provided by the upgrade. Tom and the engineers meet regularly during the evaluation period to discuss and compare their experiences. In addition, Tom asks the engineers (or a consultant, if the engineers don't have the appropriate knowledge) to double-check his work in installing NetWare 5.1. This approach ensures that the test provides a fair trial of the software.

4. Training—Judging by the results of the initial stages of evaluation, Tom predicts that his company will purchase the upgrade. To prepare for this event, he sends the networking engineers to NetWare 5.1 training. He also recommends training for the help desk personnel. In addition, Tom discusses possibilities for user training with the company's computer training manager. Most importantly, he signs up for NetWare 5.1 training himself, because he will actually perform the upgrade. He schedules his training to take place only a few weeks before the anticipated implementation date so that his new skills will be fresh when he begins the conversion.

5. Pre-implementation—As the first step of implementation, Tom expands on the rough timeline and plan that he created in his proposal. The result is a full-fledged project plan for the upgrade. He plans the transfer of the IDs, groups, and their rights to the new system. He decides how he would like to reorganize the NetWare NDS tree and what types of volumes to create. In addition, Tom reviews the existing servers to determine which applications, files, and directories should be transferred and which can be archived. He plans to upgrade the operating system on only one server at a time.

   Two weeks before upgrading the first server, Tom informs users, help desk personnel, and other networking staff of the timeline and explains what changes to expect. He recommends to users that they clean up their data directories on the server and discard any unnecessary files. Similarly, he asks networking staff to remove any unnecessary applications or services they have installed on the server. If necessary, he and his staff arrange to upgrade the client software on all workstations that will be affected by the operating system upgrade. A few days before the upgrade, he issues a final warning to staff specifying how long he will have the server down to accomplish the upgrade.

6. Implementation—Tom decides to implement the upgrade over a weekend. Before beginning the process, he gathers the software documentation and his plan, along with the software CDs and a bootable disk for the server (making certain that the CD-ROM device driver is on the bootable disk). At 7:00 P.M. on Saturday, he sends a broadcast warning to all users on the network that the server will be going down in five minutes. Five minutes later, he disables all logins to the network. He then backs up the entire server to a tape drive. When the backup is complete, he uses his backup software to verify that critical files were successfully copied.

   Once he's certain that the backup worked, Tom starts the server with DOS and follows Novell's instructions for upgrading from NetWare version 4.11 to version 5.1. This process may take an hour or more. After the upgrade finishes, Tom configures the server according to Novell's instructions and his network's specifications (for example, setting the TCP/IP parameters). Once he has added all services and configured the server properly, he enables himself (but no other users) to log in and test the server's functionality. Tom also

tests the critical applications on the server as well as the server's connectivity with the rest of the systems and devices on the network. Not only does he test the network using his (privileged) ID, but Tom also tests it using an average client's ID.

7. Post-implementation—After he is satisfied that the network operating system upgrade was successful, Tom reenables logins to the network and informs all staff that the system is running again. He and his staff review the upgrade process to see if they learned any lessons that could make the other server upgrades more efficient and less troublesome. They work with the help desk personnel to understand the kinds of support calls generated by the upgrade. They also continue testing the new operating system, fine-tuning when necessary, to fix problems or find errors before they become problems for users.

Unfortunately, the careful process of evaluation, planning, and implementation described in these steps rarely reflects reality. Most network administrators are too busy to perform all of these functions themselves. With some foresight, however, they can strive to perform most of these steps and save themselves the consequences of poor planning during or after the operating system is upgraded.

Reversing a Software Upgrade

If the software upgrade you perform creates problems in your existing system, you should be prepared to reverse the process. The process of reverting to a previous version of software after attempting to upgrade it is known as **backleveling**. Every network professional has been forced to backlevel at some point in his or her career. The steps that constitute this process differ depending on the complexity of the upgrade and the network environment involved.

Although no hard and fast rules for backleveling exist, Table 13-1 summarizes some basic suggestions. Bear in mind that you must always refer to the software vendor's documentation to reverse an upgrade. If you must backlevel a network operating system upgrade, you should also consult with experienced professionals about the best approach for your network environment.

Table 13-1 Reversing a software upgrade

Type of Upgrade	Options for Reversing
Operating system patch	Use the patch's automatic uninstall utility
Client software upgrade	Use the upgrade's automatic uninstall utility or reinstall previous version of the client on top of the upgrade
Application upgrade	Use the application's automatic uninstall utility or maintain complete copy of the previous installation of the application and reinstall it over the upgrade
Operating system upgrade	Prior to the upgrade, make a complete backup of the system; to backlevel, restore entire system from the backup; uninstall an operating system upgrade only as a last resort

HARDWARE AND PHYSICAL PLANT CHANGES

Hardware and physical plant changes may be required when a network component fails or malfunctions, but more often they are performed as part of an upgrade to increase capacity, improve performance, or add functionality to the network. In this section, you will learn about the simplest and most popular form of hardware change—adding more of what you already use, such as adding four more switches to the backbone or adding 10 new networked printers. You will also learn about more complex hardware changes, such as replacing the entire network backbone with a more robust system.

Many of the same issues apply to hardware changes as apply to software changes. In particular, proper planning is the key to a successful upgrade. When considering a change to your network hardware, use the following steps as a guide:

1. Determine whether the change is necessary.
2. Research the upgrade's potential effects on other devices, functions, and users.
3. If you decide to implement the change, notify system administrators, help desk personnel, and users and schedule it during off-hours (unless it is an emergency).
4. If possible, back up the current hardware's configuration. Most hardware (for example, routers, switches, and servers) has a configuration that you can easily copy to a disk. In other cases (for example, networked printers), you may have to print out the hardware's configuration.
5. Prevent users from accessing the system or the part of the system that you are changing.
6. Keep the installation instructions and hardware documentation handy.
7. Implement the change.
8. Test the hardware fully after the change, preferably putting a higher load on the device than it would incur during normal use in your organization. Note any unintended or unanticipated consequences of the change.
9. If the change was successful, reenable access to the device. If it was unsuccessful, isolate the device or reinsert the old device, if possible.
10. Inform system administrators, help desk personnel, and users when the change is complete. If it was not successful, explain why.
11. Record your change in the change management system.

Adding or Upgrading Equipment

The difficulty involved in adding or upgrading hardware on your network will depend largely on whether or not you have used the hardware in the past. For instance, if your organization always uses Intel hubs, adding one more Intel hub to your second-floor

telecommunications closet may take only a few minutes and cause absolutely no disruption of service to your users. On the other hand, even if your company uses Intel hubs, adding an Intel router to your network may be an entirely new experience. You should research, evaluate, and test any unfamiliar piece of equipment that you intend to add or upgrade on your network, even if it is manufactured by a vendor that supplies much of your other hardware.

With the rapid changes in the hardware industry, you may not be able to purchase identical hardware even from one quarter to the next. If consistency is a concern—for example, if your technical staff is familiar with only one brand and model of printer, and you do not have the time or money to retrain personnel—you would be wise to purchase as much hardware as possible in a single order. If this approach is not feasible, purchase equipment from vendors with familiar products and solid reputations.

Each type of device that you add or upgrade on the network will have different preparation and implementation requirements. Knowing exactly how to handle the changes will require not only a close reading of the manufacturer's instructions, but also some experience with the type of networking equipment at hand. The following list provides a very general overview of how you might approach adding or upgrading devices on the network, from the least disruptive to the most complex types of equipment. The devices at the bottom of the list are not only the most disruptive and complex to add or upgrade, but also the most difficult to remove or backlevel.

- *Networked workstation*—A networked workstation is perhaps the simplest device to add. It directly affects only a few users but does not alter network access for anyone else. If your organization has a standard networked workstation configuration (for example, a disk image—a compressed snapshot of the workstation's contents—on the server), adding a networked workstation will be a quick operation as well. You can successfully add a networked workstation without notifying users or support staff and without worrying about down time.
- *Networked printer*—A networked printer is easy to add to your network, too. Adding this equipment is slightly more complex than adding a networked workstation, however, because of its unique configuration process and because it is shared. Although it affects multiple users, a networked printer does not typically perform a mission-critical function in an organization, so the length of time required to install one does not usually affect productivity. Thus, although you should notify the affected users of a networked printer addition, you do not need to notify all users and support staff. Likewise, you do not need to restrict access to the network or worry about down time in this instance.
- *Hub*—As you learned in Chapter 6, a single hub may service as few as 4 or as many as 64 users. You do not have to worry about down time or notifying users when adding a new hub, however, because it cannot affect anyone until it is actually in use. If you are upgrading or swapping out an existing hub, you must notify the affected users. The upgrade or swap will create down time;

you may have to perform the operation during off-hours. In addition, you must consider the traffic and addressing implications of adding or upgrading a hub. For example, if you need to expand the capacity of a TCP/IP-based network segment from 24 users to 60 users, you can easily enough swap your 24-port hub with a 64-port hub. Before doing so, make sure that the segment has enough free IP addresses to service 60 users; otherwise, these users will not be able to access the network.

- *Server*—A server addition or upgrade can be tricky. Typically, this type of change (unless it is the replacement of a minor component) requires a great deal of foresight and planning. Before installing a new server, you need to consider the hardware and connectivity implications of the change, as well as issues relating to the network operating system. Even if you are adding a server that will not be used immediately, you still need to plan for its installation. Preferably, you should add the server while network traffic is low or non-existent. You should also restrict access to the servers; otherwise, one of your users could find the server while browsing the network and try to save files to it or run an application from it.

  Upgrading the hardware (such as a NIC or memory) on an existing server requires almost the same amount of planning as adding an entirely new server. You should schedule upgrades to an existing server for off-hours, so that you can shut down the server without inconveniencing any users who rely on it.

- *Switches and routers*—Switches and routers are the most complex type of additions or changes to a network design for several reasons. First, they can be physically disruptive—that is, they often require the installation of new racks or other support frames in your telecommunications room. Second, they affect many users—perhaps all users—on the network. For instance, if you must replace the Internet gateway for your organization's headquarters, you will cut every user's access to the Internet in the process (unless you have redundant gateways, which is the optimal setup if you rely on the Internet for mission-critical services). You should notify all users on the network about the impending change, even if you don't think that they will be affected—sometimes a router or switch may have unintended effects on segments of the network other than the one it services. In addition, you should plan at least weeks in advance for switch or router changes and expect at least several hours of down time. Because routers and switches are expensive, you should take extraordinary care when handling and configuring the equipment. Also, because switches and routers serve different purposes, rely on the manufacturer's documentation to guide you through the installation process.

The best way to safely gain experience with adding, upgrading, or repairing devices is to experiment with devices that are not currently used on a network. If you are taking a networking class, ask your instructor whether you can spend extra time in the computer lab polishing your skills with the equipment. Work with a partner, if possible, so you can question each other about what you are doing and why.

Bear in mind that adding a new processor to a server, a new NIC to a router, or more memory to a printer may affect your service or warranty agreement with the manufacturer. Before purchasing any components to add or replace in your network devices, check your agreement for stipulations that might apply. You may be allowed to add only components made by the same manufacturer or risk losing all support from that manufacturer.

Above all, keep safety in mind when you upgrade or install hardware on a network. Never tinker with the insides of a device that is turned on. Make sure that all cords and devices are stowed safely out of the way and cannot cause trips or falls. Avoid wearing jewelry, scarves, or very loose clothing when you work on equipment; if you have long hair, tie it back. Not only will you prevent injury this way, but you will also be less distracted. By removing metal jewelry, you may prevent damage to the equipment caused by a short if the metal touches a circuit. If the equipment is heavy (such as a large switch or server), do not try to lift it by yourself. Finally, to protect the equipment from damage, follow the manufacturer's temperature, ventilation, antistatic, and moisture guidelines.

Cabling Upgrades

Cabling upgrades (unless they involve the replacement of a single faulty patch cable) may require significant planning and time to implement, depending on the size of your network. Remember from Chapter 12 that troubleshooting cabling problems may be difficult because the cable layout may be undocumented and poorly planned, particularly if it was installed years before and survived intact despite building changes and network growth. For the same reason, cabling is rarely simple to upgrade. The best way to ensure that future upgrades go smoothly is to carefully document the existing cable *before* making any upgrades. If this assessment is not possible, you may have to compile your documentation as you upgrade the existing cabling.

Because a change of this magnitude will affect all users on the network, you should upgrade the network cabling in phases. Perhaps you can schedule an upgrade of the first-floor east wing of your building one weekend, then the first-floor west wing of your building the next, and so on. Weigh the importance of the upgrade against its potential for disruption. For example, if the Payroll department is processing end-of-month checks and having no difficulties other than somewhat slow response time, it is not critical to take away its access to install CAT5 wiring. On the other hand, if the building maintenance staff needs a 100-Mbps connection to run a new HVAC controls system, you will probably make it a priority to take down this access temporarily and replace the wiring. In this case, not only will you have to replace the wiring, but you may also need to replace hubs and NICs.

For the most part, only organizations that run very small networks upgrade or install their own network cabling. Most other organizations rely on contractors who specialize in this service. Nevertheless, as a networking professional you should know how to run a cable across a room, either under a raised floor or through a ceiling, in order to connect a device to the network.

Backbone Upgrades

The most comprehensive and complex upgrade involving network hardware is a backbone upgrade. Recall from Chapter 5 that the network backbone represents the main conduit for data on LANs and WANs, connecting major routers, servers, and switches. A backbone upgrade requires not only a great deal of planning, but also the efforts of several personnel (and possibly contractors) and a significant investment. You may upgrade parts of the backbone—a NIC in a router or a section of cabling, for example—at any time, but upgrading the entire backbone changes the whole network.

Examples of backbone upgrades include migrating from Token Ring to Ethernet, migrating from Ethernet to ATM, migrating from a slower technology to a faster one, and replacing all routers with switches (to make use of VLANs, for example). Such upgrades may satisfy a variety of needs: a need for faster throughput, a physical move or renovation, a more reliable network, greater security, more consistent standards, support of a new application, or greater cost-effectiveness. For example, switching from Token Ring to Ethernet may make a LAN less expensive to maintain because Ethernet's components are more economical and technical support may be easier to find. The need for faster throughput may prompt an upgrade from an older Ethernet technology to Gigabit Ethernet. Likewise, the need to support videoconferencing may require a backbone upgrade from CAT5 to fiber and from Ethernet to ATM.

If you recall from Chapters 4 and 6 the cabling and hardware required for the different networking technologies, you will get an idea of how far-reaching a backbone upgrade can be. For example, to convert from Token Ring to Ethernet, you must replace or upgrade connectivity equipment such as hubs and routers. In addition, you must replace the NIC in every workstation and printer on the network and change the configuration for each device so that it works with Ethernet rather than Token Ring. For a small network, this effort may not be more than a weekend's work. For a network of thousands of users, such an upgrade requires the services of a dedicated team.

Because backbone upgrades are expensive and time-consuming, the first step in approaching such a project is to justify it. Will the benefits outweigh the costs? Can the upgrade wait a year or more? If so, you might be wise to wait and find out whether a cheaper or better technical solution will become available later. Don't try to wait until the technology "settles down," because networking progress never stands still. On the other hand, do wait to implement brand-new technology until you can find out how it has worked on other networks similar to your own or until the manufacturer eliminates most of the bugs.

The second step is to determine which kind of backbone design to implement. To make this decision, you must analyze the future capacity needs of your network, decide whether you want a distributed or collapsed backbone, discover whether you want to rely on switches or routers, decide whether to use subnetting and to what extent, and so on. Although some of these predictions will be guesswork, you can minimize the variables by examining the history of your organization's growth and needs. This effort is where your baselining proves valuable.

For example, if you work with a retailer that opened 15 new stores across the country this year and predicts a growth rate of 30% over the next 5 years, you can predict that your WAN will grow by approximately 20 nodes next year and approximately 27 nodes the following year. You should plan a network upgrade that can accommodate that growth: one that uses a reliable service provider, an addressing scheme that can be expanded, and connectivity devices that can be upgraded easily.

After designing your backbone upgrade, you should develop a project plan to accomplish the upgrade. Given that you don't upgrade your backbone every day, you might want to contract this work to a firm that specializes in network design and upgrades. In that case, you will draft a request for proposal (RFP) to specify what that contractor should do. (Drafting an RFP is just one step in managing a large networking project. You will learn more about this process in Chapter 16, "Managing Network Design and Implementation.")

Regardless of whether you employ specialists, your project plan should include a logical process for upgrading the backbone one section at a time (if possible). Because this process will cause network outages, determine how best to proceed based on users' needs. If you are lucky, you will choose a time when usage is low (such as over a holiday) to perform your upgrade.

Reversing Hardware Changes

As with software changes, you should provide a way to reverse the hardware upgrade and reinstall the old hardware if necessary. If you are replacing a faulty component or device, this restoration will, of course, not be possible. If you are upgrading a component in a device, on the other hand, you should keep the old component safe (for example, keep network interface cards in static-resistant containers) and nearby. Not only might you need to put it back in the device, but you might also need to refer to it for information. For example, if you have not documented the necessary jumper settings for an interface card in a switch, the old card might indicate the jumper settings needed on your new card. Even if the device seems to be operating well with the new component, keep the old component for a while, especially if it is the only one of its kind at your organization.

Managing Growth and Change

One of the most challenging and exciting aspects of being a networking professional is keeping up with the myriad changes in the industry. Technology trends come and go, as do software and hardware suppliers. Because no one can predict the future, you must learn to do the next best thing—prepare for the future. You will not always make the right decisions, but understanding the history of networking trends and researching possibilities for the future ensure that you can make well-reasoned decisions. The following sections will help you decide how to manage your organization's networking needs.

Trends in Networking Technology

You have probably recognized trends in networking technology while reading this book (for example, the debate over cable modem versus DSL technology for low-cost, high-bandwidth WAN connections mentioned in Chapter 7) or while working in an IT department. Switches are becoming more like routers. Older transmission media such as Thicknet and Thinnet Ethernet have been replaced by twisted-pair cabling. TCP/IP is becoming the protocol of choice on many networks. These trends have been developing for a long time, however. The more interesting question is, What can we learn from these trends that will help us predict new trends over the next decade?

Each of the networking trends evident today provides users with at least one of the following advantages: faster data processing and transmission, more comprehensive integration, open standards, greater accessibility for a more diverse population, or smarter devices (which facilitates more automation of tasks, usually saving time and money). Consider how each of these factors might influence currently developing trends:

- Faster data processing and transmission will bring network access to more people in less time. If you apply this trend to the Internet, you can imagine how commerce, education, and entertainment can be easily carried worldwide over the Web. Will it replace your TV or phone? Or will your TV rely on the Web?
- More comprehensive integration means that more products sold by different vendors will work well together. This compatibility not only makes your job as a networking professional easier (because you have fewer systems to master), but also merges industries. Think of how the roles of telephone companies and Internet service providers are converging. ISPs are now selling voice over IP services, whereas telephone companies are providing Internet access over their networks.
- Open standards (as described in Chapter 10) will make networking careers less specialized and probably more interesting. With TCP/IP networking skills, for example, you could just as easily get a job with a large aerospace firm as you could with an organic food coop.
- Greater accessibility will bring technology to more users. In the 1950s, computers were used only by elite computer scientists and a single computer didn't even fit into one room. Today, the majority of U.S. households own a computer, and millions of users are connected around the world through the Internet. How might this trend affect the global economy? How might it affect cultures and political systems around the world?
- Smarter devices will contribute to each of the trends mentioned above, enabling the development of faster, more open standards and providing greater accessibility. For example, advanced wireless devices now enable users to pick up their e-mail from handheld devices while sipping coffee at an outdoor café.

Notice that lower cost is not necessarily a driving factor in networking technology trends. It doesn't have to be, because the trend toward smarter, faster, and more standardized devices also implies lower costs. Because networking equipment develops so rapidly, today's expensive and powerful devices become tomorrow's inexpensive commodities.

Some of the current trends will bring a greater concern for security. As systems adopt the same (open) standards, they become more vulnerable to hackers who can easily figure out the code after mastering similar systems. As accessibility increases, security threats also increase, because the network offers more entry opportunities for hackers. In Chapter 15, you will learn about protecting data from the unintended consequences of business's increasing reliance on the networking trends discussed above.

Researching Networking Trends

If you are charged with purchasing or planning decisions in your IT department, you will need to research networking technology trends before making any choices. Often you will hear about new technologies from colleagues, classmates, or trade magazine articles, but you cannot rely on the accuracy of everything you hear. The best way to evaluate networking technology is to test it in your organization. That way you can find out how it operates in your networking environment—with your equipment, applications, and users. During the testing, you can note what you like or don't like and decide whether you even need the technology.

On the other hand, many networking trends require such drastic or expensive upgrades that you cannot afford to test them first. In this case, you must rely on someone else who has experience with the technology. A good option is to discuss your needs with a reputable consulting firm that has implemented the same technology at other organizations. Discuss the project not only with the consultants who performed the upgrade work, but also with the customer that is currently using the new technology. If possible, visit facilities that have already adopted the technology.

Newsgroups on the Web can provide valuable information, too. After a new technology has been marketed for a month or more, you should be able to find comments from other networking professionals regarding their experience with the technology. Post a message to the newsgroup inquiring about the technology's pros and cons. Most technicians will happily share their experiences. If the technology works as promised, they will undoubtedly want to spread the good news. If it causes more problems than it solves, they will want to warn others. As you read the postings on a newsgroup, one message will come through loud and clear: Don't rely on the manufacturer's claims regarding the merits of a particular product or service. Instead, test the technology yourself, or at least discuss it with someone who has tested it.

CHAPTER SUMMARY

- In every aspect of networking, keeping accurate and updated documentation will reduce troubleshooting time and help you manage the network more effectively. When maintaining the network, you should track all changes and upgrades that you perform, as well as the state of the network before and after the changes were implemented.
- The practice of measuring and recording your network's current state of operation is called baselining. Baselining measurements may include the utilization rate on your network backbone, the number of users per day or per hour, the number of protocols run on your network, statistics about errors (such as runts, collisions, jabbers, or giants), the frequency with which networked applications are used, or the identification of those users who take up the most bandwidth.
- Baseline measurements allow you to compare future performance increases or decreases due to network changes with past network performance. Baselining offers the only way to discern whether your upgrades or changes really helped or harmed the level of service.
- Baselining can also help you predict the effect of a significant network change. When you are planning system upgrades, baselining provides the best way to predict your needs.
- Baselining differs from network monitoring. A baselined characteristic can be used as a gauge for future reference, whereas network monitoring provides a continual check for problems on the network. These tools work well together, but they are not identical.
- An asset management system includes an inventory of the total number of components on the network as well as each device's configuration files, model number, serial number, location on the network, and a technical contact for support. In addition, it records every piece of software purchased by your organization, its version number, vendor, and technical support contact.
- You should document any changes to a network as the result of maintenance or upgrades in a change management system. This information will alert your colleagues to changes made and help you remember when you implemented them. It will also assist in baselining and network performance measurement, because you will know exactly when a network component was added, removed, or changed, and can correlate this information with performance data.
- No matter what type of software upgrade you perform, you should generally follow the same process. First, determine whether the change (whether it be a patch, revision, or upgrade) is necessary. Next, research the upgrade's purpose and potential effects on other programs. Determine whether the change should apply to all or only some users and whether it will be distributed centrally or machine-by-

machine. If you decide to implement the change, notify system administrators, help desk personnel, and users and schedule the upgrade during off-hours (unless it is an emergency). Back up the current system or software before making any changes. Prevent users from accessing the system or part of the system affected (for example, disable logins). Keep the upgrade instructions handy and follow them during installation of the patch or revision. Make the change. Test the system fully after the change, noting any unintended or unanticipated consequences. If the change was successful, reenable access to the system. If it was unsuccessful, revert to the previous version of the software. Inform system administrators, help desk personnel, and users when the change is complete, or if you had to reverse it, explain why. Record your change in the change management system.

- A patch is an enhancement or improvement to a part of a software program, often distributed at no charge by software vendors to fix a bug in their code or to add slightly more functionality. Patches differ from revisions and software upgrades because they change only part of the software program, leaving most of the code untouched.
- Make it a policy to keep informed about patches to your network software, whether they involve the operating system, an application, or a client program. If you work in a large organization with several servers, routers, and other devices, you may want to assign one network administrator to manage patches for the servers, another to manage patches for the printers, and so on.
- A software upgrade represents a major change to the existing code, which may or may not be offered free from a vendor and may or may not be comprehensive enough to substitute for the original program. An upgrade to the client program replaces the existing client program so as to add functionality and fix bugs found in the previous version.
- Before upgrading client software, carefully read the instructions that accompany the upgrade to find out how best to apply it, whether it depends on any previous upgrades, whether it requires any special preparation, and how its changes will affect users. Client upgrades typically overwrite some system files (such as .dll files) on the workstation, so their installation may affect other programs adversely.
- Like client upgrades, application upgrades consist of modifications to all or part of a program that are designed to enhance functionality or fix problems with the software. Application upgrades, however, affect software programs shared by clients on the network.
- Perhaps the most critical type of software upgrade you'll perform comprises an upgrade to your network operating system. This effort usually involves significant, potentially drastic, changes to the operation of your servers and clients. As such, it requires plenty of forethought, product research, and rigorous testing before you implement it. In fact, for any network with more than a few users, you should create and follow a project plan for this undertaking.

- The process of upgrading a network operating system should include research, proposal, evaluation, training, pre-implementation, implementation, and post-implementation phases.
- If the software upgrade you perform causes problems to your existing system(s), you should know how to reverse the process. The restoration of a previous version of software after an attempted upgrade is known as backleveling.
- Hardware and physical plant changes may be required when your network has problems. More often, however, they are performed as part of a move to increase capacity, improve performance, or add functionality to the network.
- Research, evaluate, and test any unfamiliar piece of equipment you intend to add or upgrade on your network, even if it is manufactured by a vendor that supplies much of your other hardware. The process of implementing a hardware upgrade is very similar to that of carrying out a software upgrade, including notifying users and preparing to bring the system down during the change.
- Each type of device you add or upgrade on the network will have its own preparation and implementation requirements. Knowing exactly how to handle the changes will require a close read of the manufacturer's instructions as well as some experience with the type of networking equipment to be installed.
- A networked workstation is perhaps the simplest device to add. It directly affects only one or a few users but does not alter network access for anyone else.
- A networked printer is easily added to your network. Adding one is slightly more complex than adding a networked workstation because of its unique configuration process and because it is shared. Although it affects multiple users, a networked printer does not typically perform a mission-critical function in an organization, so the length of time required for its installation does not affect productivity.
- If you are adding a new hub, you do not have to worry about down time or notification of users. If you are upgrading or swapping out an existing hub, you must notify the affected users. The upgrade or swap will cause down time and may require that you perform it during off-hours. In addition, you must consider the traffic and addressing implications of adding or upgrading a hub.
- Installing a new server will require that you consider not only the hardware and connectivity but also the network operating system implications of the new server. Even if you are adding a server that will not be used immediately, you need to plan for its addition and preferably install it while the network has little traffic. Typically, a server addition or upgrade (unless it is the replacement of a minor component) requires a great deal of foresight and planning.
- Switches and routers are complex additions or changes to a network design for several reasons. First, they can be physically disruptive, often requiring the installation of new racks or other support frames in your telecommunications room. Second, they affect many users—perhaps all users—on a network. You should notify all users

on the network about the impending change, even if you don't think that they will be affected. A router or switch can have unintended effects on segments of the network other than the one it services. In addition, you should plan at least weeks in advance for switch or router changes and expect at least several hours of down time.

- Cabling upgrades (unless they involve the replacement of a single faulty patch cable) may require significant planning and time to implement, depending on the size of your network. Because an upgrade of this magnitude will affect all users on the network, you should upgrade the network in phases.
- The most comprehensive and complex upgrade involving network hardware is a backbone upgrade. The network backbone serves as the main conduit for data on LANs and WANs, connecting major routers, servers, and/or switches. A backbone upgrade not only requires a great deal of time to plan, but also the efforts of several staff members (and possibly contractors) and a significant investment.
- A variety of needs may drive backbone upgrades: for faster throughput, a physical move or renovation, a more reliable network, greater security, more consistent standards, support of a new application, or greater cost-effectiveness.
- Because backbone upgrades are expensive and time-consuming, the first step in approaching such a project is to justify it. The next step is to determine what kind of backbone design to implement. To make this decision, you must analyze the future capacity needs of your network, determine whether you want a distributed or collapsed backbone, decide whether you need to rely on switches or routers, decide whether to use subnetting and to what extent, and so on. After you have designed your backbone upgrade, you should develop a project plan to accomplish it.
- You should provide a way to reverse the hardware upgrade and replace it with the old hardware. If you are upgrading a component in a device, keep the old component safe (for example, keep NICs in static-resistant containers) and nearby. Not only might you need to put it back in the device, but you might also need to refer to it for information.
- Each of the networking trends observed today provides users at least one of the following advantages: faster data processing and transmission, more comprehensive integration, open standards, greater accessibility for a more diverse population, or smarter devices (which increases the automation of tasks, usually saving time and money).
- Some of the current trends will raise greater concerns for security. As systems adopt the same (open) standards, they become more vulnerable to hackers who can easily figure out the code after mastering similar systems. As accessibility increases, security threats also increase, because the network offers more entry opportunities for hackers.

- The best way to evaluate networking technology is to test it in your organization. That way you can find out how it operates in your networking environment—with your equipment, applications, and users. Another good option is to discuss your needs with a reputable consulting firm that has implemented the same technology at other organizations. Discuss the project not only with the consultants who performed the upgrade work, but also with the customer that is currently using the new technology. If possible, visit facilities that have already adopted the technology.

KEY TERMS

asset management — A system for identifying and tracking the hardware and software on a network.

backleveling — The process of reverting to a previous version of a software program after attempting to upgrade it.

baselining — The practice of measuring and recording a network's current state of operation.

bug — A flaw in software or hardware that causes it to malfunction.

patch — A correction, improvement, or enhancement to part of a software program, often distributed at no charge by software vendors to fix a bug in their code or to add slightly more functionality.

service pack — A significant patch to Windows NT or 2000 Server software.

upgrade — A major change to the existing code in a software program, which may or may not be offered free from a vendor and may or may not be comprehensive enough to substitute for the original program.

REVIEW QUESTIONS

1. Which of the following is *not* a benefit of a baselining tool?
   a. It helps predict the impact of future device additions.
   b. It helps predict bandwidth needs.
   c. It helps determine how much traffic currently travels over the network.
   d. It helps determine where additional WAN nodes ought to be located.
2. Name three network characteristics that might belong in a baseline measurement.
3. If you were planning to purchase a baselining tool for your network, which of the following is one factor you would *not* use to evaluate your options?
   a. interoperability with word-processing applications
   b. compatibility with network hardware and software
   c. measurement of data critical to your network's performance
   d. ease of use

4. What hardware-related data might you record in an asset management system and why?
5. Some asset management programs can automatically discover all devices on a network. True or False?
6. Which of the following times would be the best time to install a patch to your network operating system?
   a. 7:00 A.M. on Monday
   b. 6:00 P.M. on Wednesday
   c. 1:00 A.M. on Sunday
   d. 2:00 P.M. on Friday
7. How does a software patch differ from an upgrade?
   a. A patch is more comprehensive than an upgrade.
   b. A patch is more current than an upgrade.
   c. A patch only fixes bugs, while an upgrade fixes bugs and upgrades old files.
   d. A patch usually changes fewer files than an upgrade.
8. Under what circumstances should network administrators inform users of software changes?
   a. always
   b. when the change might affect applications or utilities relied on by the users
   c. when the change might result in the addition of an application
   d. when the change might affect how users are added to the system
9. Name five considerations that you should address before undertaking a network operating system upgrade.
10. When considering a major upgrade, such as a network operating system or backbone upgrade, you should depend on a manufacturer's Web site materials to determine whether the upgrade is necessary and useful. True or False?
11. What is another name for reversing a software upgrade?
    a. uninstalling
    b. backleveling
    c. reverting
    d. undoing
12. Which of the following is the best way to reverse a network operating system upgrade?
    a. Reinstall the previous version of the operating system.
    b. Uninstall the upgrade.
    c. Remove the upgrade software folder from the server.
    d. Restore the server's software and configuration from a backup.

13. Name three reasons to perform a hardware upgrade on a network.
14. Which of the following changes probably requires the most planning?
    a. modifying a router's access list
    b. upgrading the network client on a department's workstations
    c. replacing a router with a switch
    d. applying a patch to a networked application
15. You can assume that installing a switch from one manufacturer is similar to installing a hub from the same manufacturer. True or False?
16. Why are cabling and backbone upgrades often implemented in phases?
17. What is the first step in a backbone upgrade?
    a. Justify it.
    b. Create a project plan.
    c. Determine its effect on users.
    d. Determine its effect on routing traffic.
18. Name two good reasons to perform a backbone upgrade.
19. Which of the following networking trends makes security a greater concern for network managers?
    a. greater network accessibility
    b. faster devices
    c. smarter devices
    d. increased use of wireless technology
20. Which of the following is the best way to research a new networking technology you are considering adapting?
    a. Ask friends about it.
    b. Read articles about it.
    c. Test it in your organization.
    d. Based on what you read, create a hypothetical scenario for the technology in your environment.

HANDS-ON PROJECTS

Even though you may not be in a position to upgrade your company's entire network backbone, you will probably have to upgrade software and hardware components on a regular basis. From these smaller upgrades and the troubles you encounter in their implementation, you can learn about more complex types of upgrades. In the next three Projects, you will perform minor software and hardware upgrades and use the information you learn to prepare

for a hypothetical major network upgrade. For these exercises, you will need a Windows 98 or Windows 2000 Professional computer with Web access that is connected to a Windows 2000 server. You will need administrator-equivalent rights on the server. The server should have at least 710 MB of hard disk space free. It should not have Service Pack 2 installed, but you should have CDs containing this patch. You should also have a Windows 2000 Server CD and a blank floppy disk. For the hardware upgrade exercise (Project 13-2), you should have a memory chip compatible with your server's hardware and space in your server to accept additional memory.

Project 13-1

In this exercise, you will install Service Pack 2 (SP2) to a working Windows 2000 server, paying attention to the patch's effects on users and applications.

1. Before you install SP2 on your Windows 2000 server, you need to find out what it does and how it will change your system. Search Microsoft's Web site to find the features of SP2 (you will find the link at **www.microsoft.com/windows2000/downloads/default.asp**). On a separate piece of paper, list five changes made by this patch. What types of improvements do the changes entail?
2. Now that you know what SP2 is supposed to achieve, research it a little more to find out whether it will be truly beneficial to your network. You can do this by searching through technical trade magazine articles to find out what others have said about SP4. Point your browser to these URLs: **www.techweb.com/search/advancedsearch** and **www.zdnet.com**. Perform searches on the term **service pack 2** at both sites. If you have the option, search the magazine sites for the term according to its relevance in the article, rather than according to the date of the article (for example, at the Techweb site, deselect the **Sort results by date** option). Note that you may have to sift through the articles to find one that concentrates on Windows 2000 SP2 (as opposed to Windows NT SP2). Does anything in the articles you find make you skeptical about performing the upgrade? Why?
3. Log on to your Windows 2000 server as an administrator equivalent and insert the SP2 CD.
4. Find the instructions for installing the service pack on the CD (in the readmesp.htm file) and study them before beginning the installation.
5. Close all applications currently running on the server.
6. To disable all logins to the Windows 2000 server, click **Start**, point to **Settings**, click **Control Panel**. The Control Panel window opens. Double-click **Administrative Tools**, then double-click **Services**. In the list of Services, right-click **Server** and choose **Stop** from the shortcut menu. Click **Yes** to confirm that you want to disable logins, then close the Service console and Control Panel.
7. In this step you will create an emergency repair disk to ensure that you have a good copy of the server's configuration in case the software installation (or later backleveling) causes problems. To create an emergency repair disk, click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, then click **Backup**.

8. The Backup window opens. Click **Emergency Repair Disk**.
9. The Emergency Repair Diskette dialog box appears. Check the check box that indicates you also want to back up the Windows registry to the hard disk. Insert a blank, formatted, floppy diskette into your floppy disk drive, then click **OK** to continue.
10. Wait while the system data is copied to your disk.
11. Once the configuration files are copied to your floppy disk, click **OK** to close the Repair Disk Utility, then close the Backup utility. Now that you have a good copy of your server's configuration, you can install SP2 by following the instructions that came with it.
12. Start the SP2 installation, following the prompts on your screen. At the Begin Installation screen, choose the **Backup files necessary to uninstall this Service Pack at a later time** option. You should always create an uninstall folder when you install service packs. In the case of SP2, you need 270 MB of space to create the uninstall folder.
13. After the service pack has finished installing, restart the Windows 2000 server and remove the service pack CD from the CD-ROM drive. The Windows 2000 Server service will restart to enable users to log in.
14. Log on to the server as the administrator. Do you receive any messages notifying you that the service pack was installed or that certain features have changed?

Project 13-2

In this exercise, you will add memory to your Windows 2000 server. If you are familiar with PC technology, you know that each machine has its own physical memory requirements. Figure 13-2 shows some popular types of memory modules (or chips).

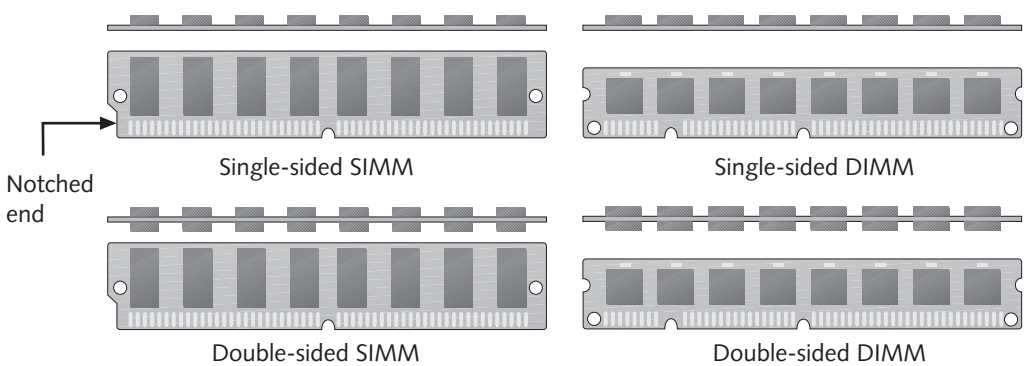

Figure 13-2 Popular memory chips

1. Log on to the Windows 2000 server as the administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, then click **Computer Management**. The Computer Management window opens.

3. Double-click the **System Information** icon. Click the **System Summary** folder.
4. The system information appears in the right-hand pane of the Computer Management window. Note the amount of Total Physical Memory installed in your server.
5. Before taking down the server to perform a memory upgrade, you must ensure that no users are currently connected. At the Computer Management console, double-click the **Shared Folders** folder. Then double-click the **Sessions** folder. Assuming that no users are connected, you can shut down the server. Otherwise, you could use the **Action – Disconnect All Sessions** option from the main menu to terminate these users' connections. Close the Computer Management console.
6. Click **Start**, then click **Shut down** to shut down the server. Make certain that the Shut down option is selected in the drop-down dialog box, then click **OK**.
7. Turn off the server and unplug it. Detach all cables, including the monitor, network, mouse, and keyboard connectors.
8. Wear a static-dissipating wristband and use a static guard mat while you open the server's casing. Because each computer is different, you should consult with your instructor to find out how to remove the casing.
9. Once you have opened the computer, insert the new memory chip by following your instructor's instructions.
10. When you have successfully installed the chip, reattach the server's cover and reconnect the power, keyboard, network, mouse, and monitor cables.
11. Turn the server on.
12. When prompted, log on to Windows 2000 as the administrator.
13. Repeat steps 2 through 4 to find out how much memory the server now has.

Project 13-3

In this exercise, you will reverse, or uninstall, the service pack that you installed in Project 13-1. Because it is not uncommon to have to uninstall a service pack, you should always create an uninstall folder. An uninstall folder contains files that can be used to reverse (or uninstall) a patch installation or upgrade. Creating an uninstall folder is an option during the installation of a service pack. Note that you should never attempt to uninstall software (especially on a Windows-based system) by deleting the new software from the system (for example, by dragging the software's folder to the Recycle Bin). Instead, you must follow proper uninstall procedures to ensure that the software's removal will not cause harm.

1. Log on to your Windows NT 2000 Server as an administrator (if you aren't already).
2. Click **Start**, point to **Settings**, click **Control Panel**, then double-click the **Add/Remove Programs** icon.

3. Select **Windows 2000 Service Pack 2**, then click **Change/Remove**. Click **Yes** to confirm the uninstall.
4. After the removal is complete, you will be prompted to restart the server to make the changes effective. Choose **Yes**.

After removing the service pack, you will have returned all applications and services to their previous state, for better or for worse. Note that the uninstall process will not remove the newer security files installed by SP2. If you want to reinstall SP2 in the future, you will need to create another uninstall folder.

Project 13-4

In this project, you will investigate one of the most popular network baselining tools—Concord Communications' Network Health. Rather than installing the program (which is expensive), you can view Concord Communications' online demo for its product. This demo includes graphs of network performance for an imaginary LAN/WAN environment. This exercise requires a workstation with Internet access and a Web browser.

1. Point your browser to the following URL**:**
   www.concord.com/products/demos/demos.htm
2. Select the Service Providers Scenario by clicking the arrow to the right of this product's description. The Service Providers Demo opens in a new browser window.
3. The Concord Communications' Network Health demo page opens. Read about the scenarios and follow the instructions in the yellow balloons to view different types of network data that this product tracks.
4. Once you reach the "At-a-Glance" report for a WAN link, examine the different data graphs that describe network activity over a link. When is the total bandwidth utilization highest? What is the relationship between bandwidth coming in (to the service provider's site) over the link and the bandwidth going out? What is the relationship between the number of bytes per second and the bandwidth graphs?
5. Continue with the demonstration and examine the page of graphs pertaining to the Web server. Is there any correlation between the database's use of the Web system's resources and the bandwidth levels on the link? Why might this be so?
6. Continue to investigate the Network Health demos. While doing so, consider the advantages and disadvantages of having so much information available to network administrators. Also, consider what types of reports would be important to a company that uses its network for e-commerce versus a company that uses a WAN to perform videoconferencing.

CASE PROJECTS

1. You work as one of five networking engineers in a large insurance company with 500 small offices located across the United States. The headquarters, where you work, relies on 10 Windows NT 4.0 servers with 128 MB RAM, Pentium II 333 processors, and redundant disk arrays; roughly half of these disk arrays provide remote access for field users, and the other half provide applications to headquarters. You have been migrating most of your routers to switches this year, and you run an Ethernet 100 Mbps LAN at headquarters. All of the 500 field offices have their own Windows NT servers, but the remote users often complain of poor support and slow or unreliable access to headquarters. Managers are also concerned about security and a need to update the company's intranet. Your manager is currently developing next year's budget. She tells you that she has more than $500,000 to spend on networking upgrades, both hardware and software. She asks your opinion about which items to include in the budget. How would you research your recommendations? What factors would influence you? What additional information should you gather? What kinds of immediate upgrades would you suggest, and which ones are optional or could wait another year?
2. Because one of your suggestions was to upgrade the server hardware, you have been asked to work with a database programmer to develop a customized asset management tool. This tool should track not only the basic facts about your hardware, but also the lease periods and the maintenance needs. Write a one-page request for proposal that will enable a developer to understand your needs. Explain the project's goals and indicate why you included the requirements, time frames, and necessary tasks that you did. Also, describe how the developer and you can make this tool easy to use and adaptable to future needs.
3. You have worked with a friend to upgrade the network operating system on a NetWare 4.11 server to NetWare 5.1 at his small auto repair office. His LAN consists of 1 server and 15 users who rely on the server for billing, customer service, word processing, and Internet access. You helped your friend follow the correct procedure of researching the upgrade, informing the users, creating a backup, and implementing the upgrade. You and he work from 6:00 P.M. to midnight performing the upgrade. When you start your testing at midnight, it looks as though the billing system doesn't work with the new operating system. The staff will begin coming to work at 5:00 A.M. What do you do, how do you do it, and why?